ORIGINAL

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The 29 computers (including cell phones) and storage mediums, as described in Attachment A, which are currently in FBI custody within the District of Oregon.	)	Case No. 3:25-mc-00296

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Oregon
(identify the person or describe the property to be searched and give its location):

The 29 computers (including cell phones) and storage mediums, as described in Attachment A, which are currently in FBI custody within the District of Oregon.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before March 28, 2025 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge Jolie A. Russo, via Clerk .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: March 14, 2025 at 3:55 pm Jolie A. Russo
Judge's signature

City and state: Portland, Oregon Hon. Jolie A. Russo, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:25-mc-00296	3/14/2025	N/A

Inventory made in the presence of :
N/A

Inventory of the property taken and name(s) of any person(s) seized:

The 29 computers (including cell phones), as detailed in Attachment A, were in the District of Oregon and in the FBI's posession when this warrant was signed. The warrant was served, authorizing the renewed search of these devices.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: April 15, 2025

Jaron Cookson
Executing officer's signature

Jaron Cookson, Special Agent
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched are the 29 computers[1] (including cell phones, as described below) and storage mediums which were seized on September 24, 2024, pursuant to multiple search warrants[2], from multiple residences and vehicles located at that time in the Middle District of Florida. The 29 computers, referred to collectively as the "**Target Devices**," are currently in FBI custody within the District of Oregon and include the following:

1. One iPhone with a blue back, model number A2632, assigned FBI evidence number 1B59.
2. One black RIG thumb drive, model number 7HX, M/C 210301011, assigned FBI evidence number 1B60;
3. One white Xbox, serial number 007253214517, assigned FBI evidence number 1B61;
4. One white and translucent computer tower, serial number CCE4-F131-70E6-171D-9, assigned FBI evidence number 1B62;
5. One iPhone with a black back, assigned FBI evidence number 1B49.
6. One iPhone with black back, Model A1660, assigned FBI evidence number 1B50.
7. One iPhone with a cracked and black-colored back, IMEI 356830111287710, assigned FBI evidence number 1B52.
8. One black ROG Zephyrus laptop, serial number NANRKD007151404, assigned FBI evidence number 1B54.
9. One iPhone with a silver or light blue back, assigned FBI evidence number 1B55.

---

[1] The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. The devices may be accessed and copied or mirrored.

[2] 3-24-mj-1429-MCR, 3-24-mj-1430-MCR, 3-24-mj-1434-MCR, 3-24-mj-1435-MCR, 3-24-mj-1428-MCR, 3-24-mj-1432-MCR, 3-24-mj-1433-MCR.

10. One iPhone with a black back, Model A1660, assigned FBI evidence number 1B51.
11. One white Logitech thumb drive, model G733, FCCID JNZA00080, assigned FBI evidence number 1B53.
12. One HP Omen 30 L Desktop PC, serial number 2M021458GF, assigned FBI evidence number 1B56.
13. One iPhone with a black case, assigned FBI evidence number 1B88.
14. One white Toyota card with a removable chip, assigned FBI evidence number 1B105.
15. One iPhone with a cracked and silver back, assigned FBI evidence number 1B92.
16. One black laptop with two missing keys, serial number NANRKD001159405, assigned FBI evidence number 1B95.
17. One black Skytech Gaming computer, serial number ST-473926989, assigned FBI evidence number 1B96.
18. One iPhone with a red back, assigned FBI evidence number 1B99.
19. One iPhone with a black back, assigned FBI evidence number 1B100.
20. One iPhone with a red back, assigned FBI evidence number 1B67.
21. One iPhone with a cracked blue back, assigned FBI evidence number 1B68.
22. One iPhone with a black back, assigned FBI evidence number 1B69.
23. One iPhone with a red back, assigned FBI evidence number 1B70.
24. One iPhone with a black back, assigned FBI evidence number 1B71.
25. One iPhone with a gold back and found inside a black case, assigned FBI evidence number 1B74.
26. One silver Apple Mac Book, serial number C02J9EZHQ6L4, assigned FBI evidence number 1B75.
27. One blue and gray Memorex 16GB USB, assigned FBI evidence number 1B80.
28. One black Dell laptop, service tag (S/N) C2322N2, assigned FBI evidence number 1B85.
29. One iPhone with tan or gold back, assigned FBI evidence number 1B86.

ATTACHMENT B

Particular Things to Be Seized

1. The items to be searched for, seized, and examined, are the 29 computers (including cell phones, as defined below) and storage mediums described in Attachment A and referred to collectively hereinafter as the "**Target Devices**," which are currently in the FBI's custody within the District of Oregon, and which contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1201(c), Conspiracy to Kidnap; and 18 U.S.C. § 1201(a)(1), Kidnapping (collectively referred to as the "Target Offenses"). These items can be searched whether or not they are stored in property packaging, are in any container or safe, or are locked or unlocked. The FBI is authorized to search for, seize, and examine the following information from September 24, 2023, through the date of execution of the warrant.

2. The items to be seized pursuant to this warrant includes records, communications (e.g., "chat messages"), images, videos, contacts, financial information, and other information that are contraband, fruits of a crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime, or that relate to or constitute evidence and instrumentalities of violations of the Target Offenses, including the following:

3. Images, videos, etc., of clothing worn by Billy Cordova ("CORDOVA"), Ralph Moreno Jr. ("MORENO"), Justice Del Carpio ("DEL CARPIO"), and/or Jackson Reves ("REVES"), referred to collectively as the **Target Suspects**, as observed by investigators around the time of the Target Offenses.

4. All communications, records, documents, programs, applications or materials related to the planning, coordination, or completion of the kidnapping and/or extortion of the adult victim ("AV") described in the affidavit supporting this warrant, in violation of the Target

Offenses, including communications (e.g., “chat messages”), images, and videos that, based on training and experience, appear consistent with conspiring to commit fraudulent account takeovers or other similar criminal activity against multiple presumed victims, the relevance of which is detailed in the supporting affidavit.

5. All communications, records, documents, programs, applications or materials related to locations or identities of individuals involved in the Target Offenses.

6. All communications that investigators believe is with or about AV, whether or not his/her true name is used.

7. Records and information containing photographs, videos, and/or audio recordings related to the Target Offenses.

8. All communications, records, documents, programs, applications or materials related to bank accounts or cryptocurrency accounts/wallets used in furtherance of, or proceeds gained through the execution of, the Target Offenses (e.g., records of payments made to purchase airline tickets, cryptocurrency payments between suspected co-conspirators around the time of the Target Offenses, wallet addresses associated with these transactions, etc.).

9. Records and information about any social media, email, or other internet accounts that have been used on any seized computer, including content stored within any application contained on the device.

10. Any and all cryptocurrency, to include the following:

a. cryptocurrency hardware wallets, digital offline storage devices, cold storage devices, Mnenomic phrases, passwords, encryption keys and seed recovery lists;

b. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

c. any and all representations of cryptocurrency private keys, whether in electronic or physical format;

d. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys" which may be used to regenerate a wallet;

e. PGP keys and/or encryption passwords or keys of any kind.

11. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

12. The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the defendant's wallets as a result of transactions that were not yet completed at the time that the defendant's devices were seized.

13. Evidence of who used, owned, or controlled any computer or storage medium at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;

14. Evidence of software that would allow others to control any seized computer or storage medium, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software, and evidence of the lack of such malicious software.

15. Evidence indicating how and when any computer or storage medium was accessed or used to determine the chronological context of access, use, and events relating to Target Offenses and to the user(s).

16. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from any seized computer.

17. Evidence of the times any seized computer was used.

18. Passwords, encryption keys, and other access devices that may be necessary to access any seized computer.

19. Records and information about any seized computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

20. Contextual information necessary to understand the evidence described in this attachment.

21. Routers, modems, and network equipment used to connect computers to the Internet.

DEFINITIONS

22. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

/ / /

23. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

24. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

SEARCH PROCEDURES

25. All evidence is to be seized for the time period from September 24, 2023, through the date of execution of the warrant, except that attribution evidence may be for any period of time through the date of the execution of the warrant.

26. The examination of the computers and storage mediums described herein may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the computers or storage mediums to human inspection in order to determine whether it is evidence described by the warrant.

27. The initial examination of the computers or storage mediums will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

/ / /

28. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computers or storage mediums or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

29. If an examination is conducted, and it is determined that a computer or storage medium does not contain any data falling within the ambit of the warrant, the government will return the computers or storage mediums to its owner within a reasonable period of time following the search and will seal any image of the computer or storage medium, absent further authorization from the Court.

30. The government may retain the computers or storage mediums as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computers or storage mediums and/or the data contained therein.

31. The government will retain a forensic image of the computers or storage mediums for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.